Policy: Network Security Policy

Reference Number:
8/7/2/1/6/9/ Network Security

Version: 3.0

Date:15/12/2021

Contents

1 Document Version Control

Changes:

DATE	AUTHOR	VERSION NUMBER	REVISION DETAILS
09/10/2018	Louis van Dyk	1.0	First Draft
13/11/2018	Louis van Dyk	1.1	Change applicability section 3 to include external service providers and consultants
24/06/2019	Louis van Dyk	1.2	Add responsible office section 4
05/07/2019	Louis Van Dyk	1.3	Overall format change
21/08/2019	Louis van Dyk	2.0	Change version for sign off
15/02/2021	Michael Stadler	2.1	Update policy details
16/02/2022	Louis van Dyk	3.0	Added intended audience section & Change version for sign off

Reviews:

DATE	AUTHOR	VERSION NUMBER	REVIEW DETAILS
02/09/2019	Michael Stadler	1.4	Reviewed
28/03/2022	Deidre Marais	3.0	Reviewed

Sign offs:

DATE	AUTHOR	DESIGNATION	SIGNATURE
	Andrew Coleman	Director: DSCS	Andrew Coleman Digitally signed by Andrew Coleman Date: 2022.03.29 07:55:23 +02'00'
	Augi de Freitas	CD: GMS	A De Freitas 2022.03.28 22:10:22 +02'00'
	Hilton Arendse	DDG: Be-I	Hilton Arendse 2022.03.30 19:57:07 +02'00'

2 Policy Overview

The WCG network spans over the local and wide area network (LAN and WAN) segments connecting end users to business applications, transversal IT services and the Internet. The WCG networks consist of a primary Corporate VPN with separate networks for Schools, Libraries and the Department of Agriculture.

The networks provide all interconnectivity and delivery of all the WCG IT services. Securing this network against external intrusion or internal abuse is therefore critical in maintaining trust and reliability.

3 Applicability

This policy applies to all individuals that provide and manage IT resources and services under the custodianship of the WCG or sourced from 3rd party services. This includes all WCG employees, third parties, temporary staff, contractors, external service providers and consultants.

3.1 Intended Audience

This policy is intended for review by all **IT operational Teams**.

The following are the key expectations of users:

- To familiarise themselves with this policy and all other related policies, standards and guidelines (where applicable).
- Take responsibility for all activity related to IT accounts they have been allocated and any information they access.
- Report any accidental breach of policy or suspected misuse of WCG IT resources or fraudulent activity to their line manager.

4 Responsible Office

The WCG Be-I information Security sub-directorateowns and maintains this policy and they can be contacted with the following email address ictpolicy.ictpolicy@westerncape.gov.za

5 Policy Statement

The policy defines required network security measures for the WCG network segments and components either connected physically or via wireless.
It addresses all equipment including servers, desktops, laptops, tablets and other mobile devices, network-related equipment as well as personally-owned equipment used by staff. While this policy addresses the specific requirements of this security area, there are other related information security policies, IT policies and standards that need to be considered.

The coverage and mandate of this policy will be limited to the scope of the Be-I managed IT environment within the WCG. These IT and information security services are focused on the Corporate Virtual Private Network (VPN) used by multiple provincial departments in the Western Cape. Other IT areas may make use of this policy but enforcement is limited by the scope of IT governance and security controls.

6 Related Policy Detail

Policy Section	**6.1 Perimeter Security**
Rationale	With the advent of cloud services and expanded connectivity, the network perimeter is increasingly complex and therefore more at risk to cyber threats. A solid defence requires improved security design, incorporating industry best practices and appropriate tooling.

Policy Statements

6.1.1 Fault tolerance, backup and recovery must be considered as part of the risk assessment with appropriate designs implemented to meet the business continuity requirements.

6.1.2 Different network segments (Trust Zones) must be appropriately segregated according to the level of risk that the WCG is prepared to be exposed to. These networks must be classified into Trusted, Semi-Trusted and Untrusted networks. Isolation must be enforced between different Trust Zones.

6.1.3 Strong cryptography at minimum 256 bit and security communication protocols must be utilised to safeguard sensitive data during transmission over untrusted networks and where required on trusted networks.

6.1.4 An intrusion detection/prevention system (IDS/IPS) must be used for the detection and blocking of malware, known attack patterns and anomalous network activity.

6.1.5 An application proxy firewall must be placed between the remote user and the internal application server to hide the identity and protect the internal server.

6.1.6 Firewalling systems must be used to prevent connections and network traffic originating from segments other than the Trusted Network (i.e. untrusted networks) from terminating in the Trusted Network.

6.1.7 Untrusted network traffic must be inspected by intrusion detection/ prevention systems and pass through a firewall. The relevant actions must be enforced by these controls to ensure that malicious traffic is blocked.

6.1.8 Connections to firewalls for administration purposes must be restricted to authorised users, IP addresses/workstations and must be configured to validate the user and verify the source IP address.

6.1.9 Changes to firewall rules must be logged and the logs must identify the administrator performing the change and when the change occurred.

6.1.10 All firewall and router rules must be reviewed at least annually. Audits must cover each rule, what it is for, if it is still necessary and if it can be improved.

6.1.11 Firewall administration must be conducted over secure channels.

6.1.12 Firewall administration and configuration must be controlled, authorised and be carried out by suitably skilled resources.

6.1.13 Anti-Virus software must only be installed and configured by IT Services. Users must not disable or interfere with anti-virus software installed on any computer.

6.1.14 No computer may be connected to the network without adequate protection i.e. up to date anti-virus software being installed and activated.

6.1.15 Users must not change or delete any anti-virus software that is installed on the WCG network.

6.1.16 Provision should be made to monitor and enforce Data Loss Prevention rules as stipulated by security and the data governance function.

Related Policies and Procedures	Data Protection Policy

Policy Section	**6.2 Wireless Network**
Rationale	Through the deployment of wireless LANs, the public-facing network at the WCG has increased its footprint substantially. As a result, the risk for a cyber attack has increased dramatically. Therefore the WCG needs to ensure that all wireless networks are centrally managed and securely configured.
Policy Statements	6.2.1 Security of the Trusted wireless network must only be configured with certificate-based authentication managed by the Network Operating System (NOS) and PKI infrastructure. 6.2.2 All approved Access Points / Base Stations are subject to periodic penetration tests and audits. 6.2.3 All vulnerabilities identified through scans or penetration tests must be promptly remediated. 6.2.4 All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with approved encryption technology. 6.2.5 Unauthorised wireless access points are not permitted to connect to the WCG networks.
Related Policies and Procedures	

Policy Section	**6.3 LAN and WAN Security**
Rationale	Good network design will ensure that security best practices are implemented. Segregation of networks, strong access controls, effective firewall placement and configuration are critical components to consider.
Policy Statements	6.3.1 Monitor overall network capacity and enforce prioritisation of business-critical applications. 6.3.2 Network Admission Control capability must be in place to ensure only authorised devices can access network resources. 6.3.3 All remote access to the network shall be authenticated, logged, and restricted to minimise the risk to network assets. 6.3.4 All communications between the Corporate Network and networks with different security profiles shall be protected by a network firewall. 6.3.5 Any new network segment connecting to the corporate network must be risk reviewed and comply with all existing security policies and standards. 6.3.6 All non-production environment (i.e. Test and Dev. environments) must be logically segregated from the production environment with a firewall.

Related Policies and Procedures	

Policy Section	**6.4 Network Infrastructure Devices**
Rationale	Network infrastructure devices are often easy targets for attackers. Once installed, many network devices are not maintained at the same security level as general-purpose desktops and servers.
Policy Statements	6.4.1 Network devices must be regularly patched as new updates become available. 6.4.2 All network devices (e.g. routers, switches, firewalls, intrusion detection/ prevention systems, etc.) must be located in physically secure locations and access to these locations restricted to authorised personnel. Access rights must be audited and verified on a regular basis. 6.4.3 All network and security devices must comply with the relevant baseline configuration standards. 6.4.4 All network and security devices that are regarded as business-critical must be configured to have highl availability. 6.4.5 All network devices must be monitored 24 x 7 for performance, availability and capacity. 6.4.6 Bi-annual security penetration tests must be performed by a trusted security partner and all potential security weaknesses identified to be reported to BE-I Security Team. These findings must be mitigated or remediated. 6.4.7 Security-related events must be logged and sent to the Security information event management system.
Related Policies and Procedures	ICT Standards list

Policy Section	**6.5 Remote Access and Third-Party Connections**
Rationale	Direct connections from external entities are required for development, outsourced services and vendor support. The WCG security policies and controls do not extend to third party networks, these connections present a significant risk to the WCG and therefore require additional security.
Policy Statements	6.5.1 Third parties must be provided with only the minimum access necessary to perform the functions required. If possible, this should include time-of-day restrictions to limit access to only the hours when such access is required. 6.5.2 All connections must have business and system owners who carry the overall accountability for the risk management of their third-party connections and accept responsibility to ensure connections are

	managed securely according to the Logical Access Management Policy. 6.5.3 For connections where strict data confidentiality is required, remote access devices should work through end-to-end encryption. 6.5.4 Third-party access to business systems should be restricted through an appropriate network security mechanism such as a DMZ, jump host, proxy or an authorised web service. 6.5.5 The operating system of all remote devices must be kept up-to-date by applying patches as soon as they become available to download.
Related Policies and Procedures	Logical Access Management Policy

7 Enforcement

The BE-I Security Function will verify compliance with this policy through various methods, including but not limited to, security reporting tools, internal and external audits and management feedback to the policy owner.

Violation of this policy (e.g. wilful or negligent exposure of confidential information) may result in disciplinary action which may include termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with the WCG. Additionally, employees, contractors and agents who violate this policy may be subject to civil and criminal prosecution.

8 Exception Handling

Exceptions to the guiding principles in this policy must be documented and formally approved by the relevant Accounting Officer of the department. Policy exceptions must describe:

- The nature of the exception
- Why the policy exception is required
- Risks created by the policy exception
- Evidence of approval by the Accounting Officer and Be-I Security Officer.

The IT and Enterprise Risk Management team must be notified of any exceptions having a risk impact.

9 Glossary

Term	Definition
Fault tolerance	Fault tolerance is the property that enables a system to continue operating properly in the event of the failure
Trusted Networks	Is a network of devices that are connected to each other, open only to authorized users
Semi- Trusted networks	
Untrusted Networks	situated outside the security perimeter and control of the network admin
PKI infrastructure	Public key infrastructure is a set of roles, policies, and procedures needed to create, manage,

	distribute, use, store & revoke digital certificates and manage public-key encryption.
WAN	Wide Area Network
LAN	Local Area Network
Corporate Network	The corporate network is the group of computers, devices connected together within WCG except for Agriculture and Education.
Network segment	A network segment is a portion of a computer network that is separated from the rest of the network
Baseline configuration standards	
DMZ	demilitarized zone (sometimes referred to as a perimeter network or screened subnet)
Penetration tests	A penetration test, colloquially known as a pen test, is an authorised simulated cyberattack on a computer system, performed to evaluate the security of the system

10 References

- National Institute of Standards and Technology(NIST) Special Publication 800-53, Revision 4;
- NIST Special Publication 800-128 Revision 3;
- COBIT 5;
- Information Technology Infrastructure Library (ITIL V3 Service Transition)
- ISO/IEC 27002:2013 Information technology -- Security techniques – Code of practice for information security management;
- CIS Critical Security Controls Version 7;
- SANS – Security Consensus Operational Readiness Evaluation – Firewall Checklist.